

**Notice of Allowability**

Application No.	Applicant(s)	
10/685,153	HONG ET AL.	
Examiner	Art Unit	
Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to amendment submitted 2/27/2007.
2.  The allowed claim(s) is/are 1 and 4.
3.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All
  - b)  Some\*
  - c)  None of the:
  1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
  - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1.  Notice of References Cited (PTO-892)
2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
3.  Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4.  Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5.  Notice of Informal Patent Application
6.  Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7.  Examiner's Amendment/Comment
8.  Examiner's Statement of Reasons for Allowance
9.  Other \_\_\_\_\_



KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER

### **EXAMINER'S AMENDMENT**

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Leo Lenna on 8/6/2007.

The application has been amended as follows:

Claim 1. A method of analyzing and decrypting a malicious encryption script, comprising the steps of:

classifying a malicious script encryption method into a case where a decryption function exists in malicious scripts and is an independent function that is not dependent on the external codes such as run time library, a case where a decryption function exists and is a dependent function that is dependent on external codes, and a case where a decryption function does not exist;

if the decryption function exists in malicious scripts and is the independent function that is not dependent on the external codes, extracting a call expression and a

function definition for the independent function, executing or emulating the extracted call expression and function definition for the independent function, and obtaining a decrypted script by putting a result value based on the execution or emulation into an original script at which an original call expression is located;

wherein if the dependency of the decryption function on the external codes is established by determining determined based on whether there exists the dependency of that all codes within the decryption function are dependant on the external codes, that whether actual parameters for decryption function call in all program are constants, and that whether only functions with no side effects in the decryption function are called; and

wherein no if there exists the dependency of all codes within the decryption function on the external codes is established by determining whether all codes within function  $F_i$  satisfies the following formula:

$$V_i \cap E_i = \emptyset$$

where  $V_i$  is a set of global variables defined as used in function  $F_{i5}$  and is obtained according to the following formula:

$$V_i = A_i - D_i, \text{ and}$$

$E_i$  is a set of variables defined or used in an external region of function  $F_i$  and is obtained according to the following formula:

$$E_i = U_j^V$$

$i \neq j, 0 \leq j \leq n$

where  $n$  is the number of functions defined in the script,

$F_i$  is an  $i$ -th defined function in the script ( $1 \leq i \leq n$ ),

$A_i$  is a set of all variables defined or used in function  $F_i$  ( $1 \leq i \leq n$ ),

$D_i$  is a set of all variables declared as Dim in function  $F_i$  ( $1 \leq i \leq n$ ), and

$V_0$  is a set of variables defined or used in a global region which does not belong to any function.

Please add claim 4 as follows.

Claim 4. The method according to Claim 1 wherein the external codes are run time library.

The examiner's statement of reasons for allowance may be found in the office action mailed 2/27/2007.

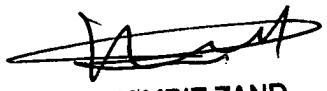
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven

  
KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER